UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,660	01/22/2004	Ron Ben-Natan	GRD03-03	5150

58406 7590 03/21/2008

BARRY W. CHAPIN, ESQ.
CHAPIN INTELLECTUAL PROPERTY LAW, LLC
WESTBOROUGH OFFICE PARK
1700 WEST PARK DRIVE
WESTBOROUGH, MA 01581

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
03/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/762,660	BEN-NATAN, RON	
	Examiner	Art Unit	
	ANDREW L. NALVEN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/19/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 are pending.

Claim Objections

2. Claims 10 and 19 are objected to because of the following informalities:

   a. Claim 10 contains the typo "the baseline includes *structure the of the access attempts*."

   b. Claim 19 contains the limitation "the parse tree" that lacks sufficient antecedent basis.

3. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 21-38 and 40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The cited claims can be interpreted to be software per se because the claims do not provide a clear limitation directed towards a physical part of a machine or device and because the claimed modules can be interpreted as wholly comprised of software. Further, with regards to claim 40, the claimed computer signal is not tangible.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-4, 7-18, 20-23, 26-27, 29-40 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Moriconi et al US Patent No. 6,941,472 in view of Lunt et al "IDES: A Progress Report."

6. **With regards to claims 1, 21, 39-40,** Moriconi teaches intercepting an access attempt to a protected resource (Moriconi, column 5 lines 45-55, grants or denies access to a resource); selectively permitting, based on the comparing, access to the resource according to the access attempt (Moriconi, column 5 lines 45-55). Moriconi fails to teach the comparison based upon previous allowable access and augment the set of allowable accesses. However, Lunt teaches comparing the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access (Lunt, page 2, right column, determines whether user behavior is normal with respect to past or acceptable behavior) and augmenting the set of allowable access attempts by selectively adding, based on

inferential feedback, the access attempt to the set of allowable access attempts (Lunt, page 2, right column, continually updates profile). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Lunt's method of using behavior statistics to determine access control decisions because it offers the advantage of helping detect intrusions that could not be detected by normal access controls and help stop attackers from exploiting a deficiency in the system's security mechanisms (Lunt, page 2, right column).

7. **With regards to claims 2, 22,** Moriconi as modified teaches comparing the access attempt determines correspondence by a matching of explicit rules qualifying allowable data access attempts and by a matching of a baseline having previously allowed data access attempts (Lunt, page 3, left column, uses expert system and subject profiles).

8. **With regards to claim 3,** Moriconi as modified teaches selectively adding, if the data access transaction corresponds to a window of allowable database activity, the data access attempt to the set of allowable data access attempts (Lunt, page 2, right column, continually updates profile).

9. **With regards to claims 4, 23,** Moriconi as modified teaches determining a structure of the access attempt corresponding to syntactical arrangement of the access attempt; and comparing the determined structure of the access attempt independently of the data values implicated in the access attempt (Lunt, page 6, categorical measure – counts similar access attempts, substance of access is not counted).

10. **With regards to claims 7, 26,** Moriconi as modified teaches defining an access policy having a plurality of access rules, the access rules indicative of allowable access, wherein the preexisting set of allowable access attempts correspond to one of the plurality of the rules (Lunt, page 3, left column, expert system and subject profiles).

11. **With regards to claims 8, 27,** Moriconi as modified teaches determining the preexisting set comprises establishing a baseline of allowable activity, the baseline indicative of an accepted set of allowable access attempts (Lunt, page 2 right column, historical profile).

12. **With regards to claim 9,** Moriconi as modified teaches the baseline is a rule in the access policy and indicates allowable access when a data access transaction matches a previous data access transaction represented in the baseline (Lunt, page 3, left column).

13. **With regards to claim 10,** Moriconi as modified teaches the baseline includes structure the of the access attempts, and avoids including data values of the data access transactions from which it is derived (Lunt, page 6, categorical measure – counts similar access attempts, substance of access is not counted).

14. **With regards to claim 11,** Moriconi as modified teaches selectively permitting further comprises computing, based on iteratively applying the access rules to the access attempt, an access result indicative of whether to allow the access attempt (Lunt, page 3 left column, Moriconi, column 5 lines 45-55).

15. **With regards to claims 12, 29,** Moriconi as modified teaches identifying a plurality of allowable access attempts; inferring, based on observable patterns in the

allowable access attempts, access rules indicative of the plurality of allowable access attempts; and adding the inferred rules to the access policy (Lunt, pages 2-3, Moriconi, column 10 lines 23-35).

16. **With regards to claims 13, 30,** Moriconi as modified teaches processing the series of allowable access attempts to determine related groups of allowable access transactions; suggesting, based on a commonality of the processed group of allowable access attempts, an access rule indicative of each of the series of allowable access attempts; and adding, in response to operator input, the suggested access rule to the access policy (Lunt, page 9 left column, page 2, adds to historical profile).

17. **With regards to claims 14, 31,** Moriconi as modified teaches a current baseline representative of a window of access attempts, further comprising modifying the current baseline by including access attempts from a different window of access attempts (Lunt, page 9 left column, active profile).

18. **With regards to claims 15, 32,** Moriconi as modified teaches identifying a sampling window of access attempts, the sampling window deterministic of allowable access patterns to the protected resource; storing an indication of the access attempts made during the window of access attempts; and merging the window of access attempts with the current baseline set of access attempts, the current baseline deemed deterministic of allowable access behavior (Lunt, page 9 left column, active profile).

19. **With regards to claims 16, 34,** Moriconi as modified teaches storing further comprises: verifying that the access attempt is indicative of allowable access behavior; and selectively adding, based on the verifying, the access attempts to the baseline of

allowable access attempts (Lunt, page 2, right column, determine if behavior is normal, if so update profile).

20. **With regards to claims 17, 35,** Moriconi as modified teaches determining the preexisting set includes comparing a sensitivity threshold indicative of a series of corresponding access attempts defining a benign pattern (Lunt, page 2, right column, significant deviation).

21. **With regards to claims 18, 36,** Moriconi as modified teaches the corresponding access attempts define a similar pattern of access structures, the access structures determined by tables and fields affected by the access attempt (Lunt, page 2).

22. **With regards to claims 20, 33,** Moriconi as modified teaches storing a set of data access attempts according to a learning window of observable database behavior; generating suggested rules; adding suggested rules to the security policy; and reanalyzing the set of data access attempts gathered during the leaning window in an iterative manner against suggested rules (Lunt, page 9 left column, page 2, adds to historical profile).

23. **With regards to claims 37, 38,** Moriconi as modified teaches an interface operable with an external application, the interface operable to transmit allowable data access attempts to the external application (Moriconi, column 5 lines 45-55).

24. **Claims 5, 6, 19, 24-25, 28 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Moriconi et al US Patent No. 6,941,472 and Lunt et al "IDES: A

Progress Report," as applied to claim 1 above, and in further view of Allen US Patent No. 6,658,625.

25. **With regards to claims 5, 6, 19, 24-25, 28,** Moriconi as modified teaches everything described above, but fails to teach the use of parse trees and the comparing of hash values. However, Allen teaches the use of parse trees and the comparing of hash values (Allen, column 12 lines 5-28, column 6 lines 47-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Allen's hashing and parse tree method because it offers the advantage of allowing the storage and easy retrieval of the parse tree and increasing efficiency of searching of the parse tree (Allen, column 6 lines 47-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Primary Examiner, Art Unit 2134